IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA
WINSTON-SALEM DIVISION

DAVID NOVACK, on behalf of himself and all others similarly situated, Plaintiff, v. **NOVANT HEALTH, INC.,** Defendant.	Case No. Judge **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff David Novack ("Plaintiff") brings this Class Action Complaint against Novant Health, Inc. ("Novant" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information and personal health information (collectively referred to herein as "Private Information"), including names, email addresses, phone numbers, computer IP addresses, and emergency contact information, appointment information, and other content submitted on Defendant's website and patient portal.

2. Novant is a healthcare provider headquartered in Winston-Salem, with fifteen (15) hospitals & more than 350 physician practices offering advanced medical treatment in the state of North Carolina. The Novant health network consists of more than 1,600 physicians and over

29,000 employees that provide care at over 640 locations. Novant treats over 5,000,000 patients annually.[1]

3. Despite Novant's status as one of the largest healthcare providers in the country, Novant failed to institute appropriate and adequate security measures to ensure the Private Information of Plaintiff's and Class Members remained secure and protected.

4. As a result of Defendant's failures, upon information and belief, Plaintiff and approximately 1,362,296 other individuals ("Class Members") have had their most sensitive personal information disclosed and exposed by Novant. [2]

5. In May 2020, Novant launched a campaign to connect more patients to the Novant Health MyChart patient portal that involved Facebook advertisements and a Meta (Facebook parent company) tracking pixel placed on the Novant Health website to help understand the success of those efforts on Facebook. A pixel is a piece of code that organizations commonly use to measure activity and experiences on their website. In this case, the pixel was configured incorrectly and may have allowed certain private information to be transmitted to Meta from the Novant Health website and MyChart portal (the "Data Breach").[3]

6. Upon becoming aware that the Facebook Pixel had the capability to transmit information to Meta, Novant disabled and removed the pixel and began an investigation to learn whether, and to what extent, information was transmitted.[4]

[1]https://www.novanthealth.org/Portals/92/novant_health/documents/about_us/mediakit/NH%202019%20Media%20Files/2019_Novant%20Health%20Fact%20Sheet.pdf
[2] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[3] https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html
[4] *Id.*

7. Based on that investigation, Novant determined on June 17, 2022, that certain Private Information of Plaintiff and Class Members was disclosed to Meta and Facebook, depending upon a user's activity within the Novant Health website and MyChart portal.[5]

8. Defendant did not disclose the Data Breach to patients until August 12, 2022, when it sent letters to Data Breach victims ("Notice of Data Breach" letter). As a result, Plaintiff and Class Members have not been properly informed that their Private Information has been disclosed.

9. Businesses that collect and store Private Information have statutory, regulatory, contractual, and common law duties to safeguard that information and ensure it remains private.

10. Plaintiff and those similarly situated relied upon Defendant to maintain the security and privacy of the Private Information they entrusted to it. Plaintiff and Class Members reasonably expected and understood that Defendant would comply with its obligations to keep the Private Information secure and safe from unauthorized access and disclosure.

11. Defendant is responsible for allowing this Data Breach through its failure to implement and maintain reasonable safeguards, its unreasonable data policies, failure to adequately train employees, and its failure to comply with industry-standard data security practices.

12. Plaintiff and members of the proposed Class have suffered actual and imminent injuries as a direct result of the Data Breach. The actual and imminent injuries suffered by Plaintiff and the proposed Class as a direct result of the data breach include: (a) theft of their personal data; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to monitor, ameliorate, mitigate and deal with the consequences of the data breach; (d) the anxiety, stress,

[5] *Id.*

nuisance, and annoyance of dealing with all issues resulting from the Data Breach; (e) actual fraudulent activity on financial and personal accounts; (f) increased fraudulent robocalls and phishing email attempts; (g) the potential for future fraud and the increased risk of identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (h) damages to and diminution in value of their personal data entrusted to Defendant; (i) the retention of the reasonable value of the Private Information entrusted to Defendant; and (j) the continued risk to their personal data which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its possession or input into its systems.

13. As a result of this delayed response from the beginning of the unauthorized disclosure until notice was provided, Plaintiff and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

14. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Plaintiff's and Class Members' Private Information; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct violates federal and state statutes.

15. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' Private Information was safeguarded,

failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding securing Private Information. As the result, Plaintiff's and Class Members' Private Information was compromised through disclosure to Meta, Facebook, and likely unknown and unauthorized third parties. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

16. Plaintiff David Novack is a citizen of South Carolina residing in Rock Hill, South Carolina.

17. Defendant Novant Health, Inc. is a corporation with its principal place of business at 2085 Frontis Plaza Blvd., Winston-Salem, North Carolina 27103.

JURISDICTION AND VENUE

18. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

19. The Middle District of North Carolina has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in North Carolina and this District through its headquarters, offices, parents, and affiliates.

20. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Background

21. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential Private Information, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

22. Plaintiff and Class Members relied on the sophistication of Defendant's healthcare business to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand proper security to safeguard their Private Information

23. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' Private Information from disclosure to third parties.

24. Defendant's Privacy Policy ("Privacy Policy") provides, "Our staff are committed to protecting your health information, which is a right you have and one detailed in the federal Health Insurance Portability and Accountability Act (HIPAA) of 1996."[6]

25. Defendant's Privacy Policy applies to any personal information provided to Novant and any personal information that Novant collects from other sources. Novant's Privacy Policy, specific for South Carolina residents also represents when Defendant will disclose Plaintiffs' and Class Members' Private Information.[7]

[6] https://www.novanthealth.org/home/privacy-statement.aspx
[7]https://www.novanthealth.org/Portals/92/Assets/Documents/Corporate/PDFs/Novant%20Health%20Notice%20of%20Privacy%20Practices%20for%20South%20Carolina.pdf

26. Defendant's privacy policy does not permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes.

27. Defendant violated its own Privacy Policy by unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook, Meta, and likely other third parties.

28. Defendant also maintains a "Digital Privacy Policy, that "applies to the websites and other mobile applications and online services which are owned, provided and operated by or on behalf of Novant Health, Inc. or its subsidiaries or majority-held joint ventures with third parties." [8]

29. The Digital Privacy Policy states, "Novant Health is committed to protecting your digital privacy. When you visit, make appointments or use Novant Health Services, you may disclose certain personal information in order to access or use some of our content and Services. This information helps us to better determine and address the healthcare needs, interests and concerns of site visitors. Some of the data you provide is considered Protected Health Information and is protected by the Health Insurance Portability and Accountability Act ("HIPAA")."

30. The Digital Privacy Policy further represents as follows:

> Novant Health provides Services through NovantHealth.org, other websites, mobile applications and voice activated assistants to serve its patients and communities. Novant Health is committed to protecting your digital privacy. When you visit, make appointments or use Novant Health Services, you may disclose certain personal information in order to access or use some of our content and Services. This information helps us to better determine and address the healthcare needs, interests and concerns of site visitors. Some of the data you provide is considered Protected Health Information and is protected by the Health Insurance Portability and Accountability Act ("HIPAA"). Our use of protected health information, as defined by HIPAA, is governed by Novant Health's Notice of Privacy Practices, and is a separate document from this Digital Privacy Policy. We may use third parties to manage our Services and the information gathered through the use of the Services.

[8] https://www.novanthealth.org/home/digital-privacy-policy.aspx

The content, products and services offered through our websites, mobile applications and voice activated assistants are provided to educate consumers on health care and medical issues that may affect their daily lives. Except for the services offered through MyChart, nothing through our Services should be considered, or used as a substitute for, medical advice, diagnosis or treatment. Our websites, mobile applications and voice activated assistants and their content and services do not constitute the practice of any medical, nursing, or other professional health care advice, diagnosis or treatment. If you choose to send information to us through one of our Services, please know that by doing so, you are not establishing a treatment relationship between you and us.

...

Novant Health collects certain information about how you reach and use our Services. This allows us to administer our systems and gather relevant information about how our Services are being used, and to deliver content relative to you and your location. We may also use this information as needed to enforce our legal rights and when required to do so by law.

. . .

We collect information about visitors to our sites using cookies and similar technology including, but not limited to, web beacons, web bugs and pixel tags. For example, "cookies" are small pieces of information that some websites store on your device when you visit some websites. A "web beacon," "clear GIF," "web bug," or "pixel tag" is a tiny graphic file with a unique identifier that is similar in function to a cookie, but would allow us to count the number of users that have visited certain pages or screens of our websites, and to help determine the effectiveness of promotional or advertising campaigns. When used in HTML-formatted email messages, web beacons can tell the sender whether and when the email has been opened. In contrast to cookies, which may be stored on your computer's hard drive, web beacons are typically embedded invisibly on pages or screens.

Like many other websites, Novant Health Services use data compiled by this tracking technology to provide us with information about traffic to our site. We use this information to personalize the experience, such as recognizing a repeat visitor in order to offer the visitor a set of services or information requested in a previous visit. For example, if you personalize a webpage, or navigate within a website, a cookie helps the website to recall your specific information on subsequent visits. This simplifies the process of delivering relevant content and eases website navigation by providing and saving your preferences and login information as well as providing personalized functionality.

We collect information about visitors to our sites using cookies and similar technology including, but not limited to, web beacons, web bugs and pixel tags. For

example, “cookies” are small pieces of information that some websites store on your device when you visit some websites. A “web beacon,” “clear GIF,” “web bug,” or “pixel tag” is a tiny graphic file with a unique identifier that is similar in function to a cookie, but would allow us to count the number of users that have visited certain pages or screens of our websites, and to help determine the effectiveness of promotional or advertising campaigns. When used in HTML-formatted email messages, web beacons can tell the sender whether and when the email has been opened. In contrast to cookies, which may be stored on your computer's hard drive, web beacons are typically embedded invisibly on pages or screens.

Like many other websites, Novant Health Services use data compiled by this tracking technology to provide us with information about traffic to our site. We use this information to personalize the experience, such as recognizing a repeat visitor in order to offer the visitor a set of services or information requested in a previous visit. For example, if you personalize a webpage, or navigate within a website, a cookie helps the website to recall your specific information on subsequent visits. This simplifies the process of delivering relevant content and eases website navigation by providing and saving your preferences and login information as well as providing personalized functionality.

We also use certain third party analytics companies to help us present information or advertising that we believe may be of interest to you based on your use of Novant Health Services. After visiting a Novant Health website, you may see information about our services on non-Novant Health websites. This may occur as a result of a placement of a cookie or other tracking technology from past browsing.

. . .

Novant Health owns or has licenses to the intellectual property rights to all components of the Services. You may use the Services only for your personal lawful purposes. Any other use of information accessed via the Services (such as reproduction, resale, publication, distribution or transmission) is not permitted.[9]

31. Defendant violated its own Digital Privacy Policy by unlawfully disclosing Plaintiffs’ and Class Members’ Private Information to Facebook, Meta, and likely other third parties.

The Data Breach

[9] *Id.*

32. On or about August 12, 2022, Defendant sent Plaintiff and Class Members a Notice of Data Breach.

33. The Notice of Data Breach informed Plaintiff and Class Members (in substantially the same form) that:

> In May 2020, as our nation confronted the beginning of the COVID-19 pandemic, Novant Health launched a promotional campaign to connect more patients to the Novant Health MyChart patient portal, with the goal of improving access to care through virtual visits and provide increased accessibility to counter the limitations of in-person care. This campaign involved Facebook advertisements and a Meta (Facebook parent company) tracking pixel placed on the Novant Health website to help understand the success of those efforts on Facebook. A pixel is a piece of code that organizations commonly use to measure activity and experiences on their website. In this case, the pixel was configured incorrectly and may have allowed certain private information to be transmitted to Meta from the Novant Health website and MyChart portal.
>
> Immediately upon becoming aware that the pixel had the capability to transmit unintended information to Meta, Novant Health disabled and removed the pixel as a precaution and began an investigation to learn whether, and to what extent, information was transmitted. Based on that investigation, Novant Health determined on June 17, 2022, that it was possible sensitive information or PHI might have been disclosed to Meta, depending upon a user's activity within the Novant Health website and MyChart portal. This information potentially included an impacted patient's: demographic information such as email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes. The information did not include Social Security numbers or other financial information unless it was typed into a free text box by the user. The letter sent to each patient will specifically state whether such financial information may have been involved.
>
> Based on its investigation, Novant Health is unaware of any improper use or attempted use of any patient information by Meta or any other third party. According to Facebook's Terms and Conditions, they have policies and filters that block sensitive personal data and do not incorporate that information into their Ad Manager. However, to be safe and transparent, Novant Health is sending letters to all potentially impacted patients, including some who are patients of independent physicians and facilities who use the Novant Health MyChart medical record. Novant Health has also implemented more structure, governance and policies around the use of pixels and is taking actions to ensure this does not happen again.

34. Defendant advised that the information potentially impacted in the Data Breach included names, email addresses, phone numbers, computer IP addresses, and emergency contact information, appointment information, and other content submitted into Defendant's website.

35. There is a potential that more information was disclosed to Meta and Facebook during the two years data was submitted to Meta from Defendant's system without detection.

36. Facebook describes itself as a "real identity platform,"[10] meaning users are allowed only one account and must share "the name they go by in everyday life."[11] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[12]

37. In 2021, Facebook generated $117 billion in revenue.[13] Roughly 97% of that came from selling advertising space.[14]

38. Facebook sells advertising space by highlighting its ability to target users.[15] Facebook can target users so effectively because it surveils user activity both on and off its site.[16] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[17] Facebook compiles this information into a

[10] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).
[11] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.
[12] FACEBOOK, SIGN UP, https://www.facebook.com/
[13] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx
[14] *Id.*
[15] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706.
[16] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.
[17] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[18]

39. Advertisers can also build "Custom Audiences."[19] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[20] With Custom Audiences, advertisers can target existing customers directly, and they can also build a "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[21] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools."[22]

40. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[23] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

---

[18] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.
[19] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.
[20] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.
[21] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328.
[22] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.
[23] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.

41. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[24] Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[25] Advertisers can even create their own tracking parameters by building a "custom event."[26]

42. One such Business Tool is the Facebook Tracking Pixel. Facebook offers this piece of code to advertisers, like Novant Health, to integrate into their website. As the name implies, the Facebook Pixel "tracks the people and type of actions they take."[27] When a user accesses a website hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's websites—Defendant's own code, and Facebook's embedded code.

43. An example illustrates the point. Take an individual who navigates to Defendant's website and clicks on a tab. When that tab is clicked, the individual's browser sends a request to

---

[24] *See* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[25] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

[26] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[27] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

Defendant's server requesting that server to load the particular webpage. Because Novant Health utilizes the Facebook Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual that this is happening. Facebook causes the browser to secretly duplicate the communication with Novant Health, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

44. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

45. Through the Facebook Pixel, Defendant Novant shares its patients' identities and online activity, including personal information and search results related to their private medical treatment.

46. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant Novant Health to disclose his Private Information and assist with intercepting their communications. Plaintiff was never provided with any written notice that Defendant discloses its website users' protected health information, nor were they provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiff's protected health information to Meta, Facebook, and unauthorized entities.

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information

47. Defendant acquired, collected, and stored the Private Information of Plaintiff and Class Members.

48. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure without authorization.

49. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for legitimate business purposes only, and to make only authorized disclosures of this information.

Plaintiff David Novack's Experience

50. Plaintiff David Novack entrusted his Private Information to Defendant as a condition of receiving Defendant's healthcare services.

51. Plaintiff accessed Defendant's website to receive healthcare services from Defendant and at Defendant's direction. Plaintiff reasonably expected that his online communications with Novant were confidential, solely between himself and Novant, and that such communications would not be transmitted to or intercepted by a third party.

52. Plaintiff provided his Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law.

53. At the time of the Data Breach, Defendant requested and retained Plaintiff's name, email address, phone number, computer IP address, and emergency contact information, appointment information, and other content submitted into Defendant's website.

54. Defendant transmitted to Facebook Plaintiff's email address, phone number, computer IP address, emergency contact information, and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes

55. On August 12, 2022, Defendant sent a Notice of Data Breach letter to Plaintiff, notifying him that Defendant improperly disclosed Plaintiff's Private Information to a third party in the Data Breach.

56. Plaintiff Novack is very careful about sharing his sensitive Private Information.

Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

57. Plaintiff Novack stores any documents containing his Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

58. Defendant Novant breached confidentiality and unlawfully disclosed Plaintiff's personally identifiable information and protected health information without his consent.

59. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff to mitigate his damages by, among other things, learning more about best practices to protect Private Information and monitoring his accounts for fraudulent activity.

60. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

61. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

62. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information,

which, upon information and belief, remain backed up in Defendant's possession, is protected, and safeguarded from future breaches.

CLASS ALLEGATIONS

63. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

64. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

65. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

66. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

67. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are 1,362,296 of individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

68. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact

common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' Private Information;

b. Whether Defendant had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for non-business purposes;

d. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' Private Information;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

69. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

70. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

71. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

72. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

73. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

74. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with

prosecuting this lawsuit as a class action.

75. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

76. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure and unlawful disclosure of the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

77. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

78. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

a. Whether a contract existed between Defendant on the one hand, and Plaintiff and

Class Members on the other, and the terms of that contract;

b. Whether Defendant breached the contract;

c. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

d. Whether Defendant breached the implied contract;

e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

79. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

80. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

81. Plaintiff and Class Members have an interested in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation,

intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to unauthorized disclosure of Private Information without Plaintiffs' and Class Members' knowledge or consent.

82. At all relevant times, by using Facebook's tracking pixel to record and communicate patient's information alongside their confidential medical communications, Novant Health intentionally invaded Plaintiff's and Class Members' privacy rights.

83. Plaintiff and Class Members had a reasonable expectation that their communications, identity, health information and other data would remain confidential when using Novant Health's website.

84. Plaintiff and Class Members did not authorize Novant Health to record and transmit Plaintiffs' and Class Members' private medical communications alongside their personally identifiable health information.

85. This invasion of privacy is serious in nature, scope, and impact because it relates to patients' private medical communications. Moreover, it constitutes an egregious breach of the societal norms underlying the privacy right.

86. Accordingly, Plaintiff and Class Members seek all relief available for invasion of privacy claims.

COUNT II
BREACH OF CONTRACT
(On behalf of Plaintiff and the Class)

87. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

88. Defendant required Plaintiff and the Class Members to provide their Private Information, including names, email addresses, phone numbers, computer IP addresses, and

emergency contact information, appointment information, and other content submitted into Defendant's website.

89. As a condition of utilizing Defendant's website and receiving services from Defendant, Plaintiff and the Class provided their Private Information. In so doing, Plaintiff and the Class entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Policies and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

90. Plaintiff and the Class Members fully performed their obligations under the contract with Defendant.

91. Upon information and belief, the Privacy Policy and Digital Privacy Policy of Defendant require it to take appropriate steps to safeguard the Private Information entrusted to it by the Plaintiff and Class Members.

92. Defendant breached these agreements, which directly and/or proximately caused Plaintiff and Class Members to suffer substantial damages.

93. Defendant breached the contracts it made with Plaintiff and the Class by failing to safeguard and protect their Private Information, and by failing to provide timely and accurate notice to them that the Private Information was compromised as a result of the Data Breach.

94. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the

compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

95. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

96. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

97. A relationship existed between Plaintiff and the Class in which Plaintiff and the Class put their trust in Novant to protect the Private Information of Plaintiff and the Class and Novant accepted that trust.

98. Defendant Novant breached the fiduciary duty that they owed to Plaintiff and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the Private Information of Plaintiff and the Class.

99. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and the Class.

100. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred.

101. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the Class.

102. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class Members are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and him counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Sensitive Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Sensitive Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant's to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

August 24, 2022

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

/s/ *Scott C. Harris*
Scott C. Harris
N.C. Bar No: 35328
900 W. Morgan Street
Raleigh, NC 27603
Telephone: (919) 600-5003
Facsimile: (919) 600-5035
sharris@milberg.com

Terence R. Coates (pro hac vice forthcoming)
Jonathan T. Deters (pro hac vice forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: 513.651.3700
Facsimile: 513.665.0219
tcoates@msdlegal.com

Counsel for Plaintiff and Putative Class